REMARKS

The Applicants and the undersigned thank Examiner Shaw for his careful review of this application. After entry of this Amendment, Claims 1-13, 15-27, 29-36, and 38-45 are pending in the present application, with Claims 1, 13, 22, 30, and 39 being independent. Applicants have amended Claims 1, 5, 13, 17, 21, 22, 24, 30, 33, 39, 40, 42, and 44 herein. Applicants have cancelled Claims 14, 28, and 37 without prejudice to, or disclaimer of, the subject matter recited therein. No new matter has been added.

Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks.

Claim Rejections

In the Office Action dated July 14, 2005, the Examiner rejected Claims 1-45 under 35 U.S.C. § 103(a). Specifically:

- The Examiner rejected Claims 30, 32, 34-35, and 37-38 under 35 U.S.C. § 103(a) as being obvious over Proctor, U.S. Patent No. 6,530,024 (hereinafter the "Proctor reference"), and further in view of Gleichauf et al, U.S. Patent No. 6,301,668 (hereinafter the "Gleichauf reference").
- The Examiner rejected Claim 31 under 35 U.S.C. § 103(a) as being obvious over the Proctor reference and Gleichauf reference as applied to Claim 30, and further in view of Hartley et al, U.S. Patent No. 6,889,168 (hereinafter the "Hartley reference").
- The Examiner rejected Claims 1-2, 4-5, 9, 11-15, 17, 20-23, 25-26, 28-29, 39, 42-45 as being obvious over the Proctor reference and further in view of the Gleichauf reference and Hartley reference.
- The Examiner rejected Claim 33 under 35 U.S.C. § 103(a) as being obvious over the Proctor reference and Gleichauf reference as applied to Claim 30, and further in view of Yang, U.S. Patent No. 6,467,002 (hereinafter the "Yang reference").
- The Examiner rejected Claims 3, 16, 27, and 41 under 35 U.S.C. § 103(a) as being obvious over the Proctor reference, Gleichauf reference, and Hartley reference as

applied to Claims 1, 13, 22, and 29, and further in view of Brabson et al, U.S. Patent No. 5,715,395 (hereinafter the "Brabson reference").

- The Examiner rejected Claim 36 under 35 U.S.C. § 103(a) as being obvious over the Proctor reference and Gleichauf reference as applied to Claim 30, and further in view of the Hartley reference and the Brabson reference.
- The Examiner rejected Claims 6-8, 18, 24, and 40 under 35 U.S.C. § 103(a) as being obvious over the Proctor reference, Gleichauf reference, and Hartley reference as applied to Claims 1, 13, 22, and 39, and further in view of the Yang reference.
- Lastly, the Examiner rejected Claims 10 and 19 under 35 U.S.C. § 103(a) as being obvious over the Proctor reference, Gleichauf reference, and Hartley reference as applied to Claims 1 and 13, and further in view of Barroux, U.S. Patent No. 6,220,768 (hereinafter the "Barroux reference").

The Applicants respectfully offer remarks to traverse these rejections. The Applicants will address each independent claim separately as the Applicants believes that each independent claim is separately patentable over the prior art of record.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the combination of the Proctor, Hartley, and Gleichauf references fails to describe, teach, or suggest: (1) conducting a discovery scan to identify an element of the computer network and determine the element's functions; (2) configuring an audit scan to perform on the element, wherein the audit scan is a more thorough scan than the discovery scan; (3) scheduling a time to perform the audit scan on the element; (4) running the audit scan of the element at the scheduled time; (5) calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element; and (6) scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan and the security score, as recited in amended independent Claim 1.

The Proctor Reference

The Proctor reference describes a system and method for managing security incidents in a computing environment that uses adaptive feedback to update security procedures in response to detected security incidents. The system and method can define security procedures, which can include one or more policies, and implement these security procedures on one or more computing systems in the computing environment. The system and method monitors activities in the environment and detects security incidents using the implemented security procedures. When a security incident is detected, the security procedures are updated in response to the detected security incident and implemented on one or more systems in the computing environment.

The Proctor reference fails to teach calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element. Proctor teaches that in accordance with the audit policy, one or more event log files can be generated and recorded indicating the various audited activities occurring within the target. See Col. 11, lines 30-33 and Step 1046 in Figure 10 of the Proctor reference below.

Next, Proctor teaches an implemented collection policy that results in the collection of records in event log files at the scheduled intervals. See Col. 11, lines 38-41 and Step 1048 in Figure 10 of the Proctor reference below. The collected records can then be provided to the security system for analysis, referred to as a security assessment. The security assessment can be performed based on the audited activities that have been recorded in event log files. See Col. 11, lines 41-45 and Step 1052 in Figure 10 of the Proctor reference below.

Finally, Proctor teaches that the security assessment determines whether an actual, attempted or potential security breach has occurred or is occurring. In response to determining that a security breach has occurred, one or more policy updates can be made to one or more of the audit policy, collection policy and detection policy. See Col. 11, lines 49-53 and Step 1054 of Figure 10 of the Proctor reference below.

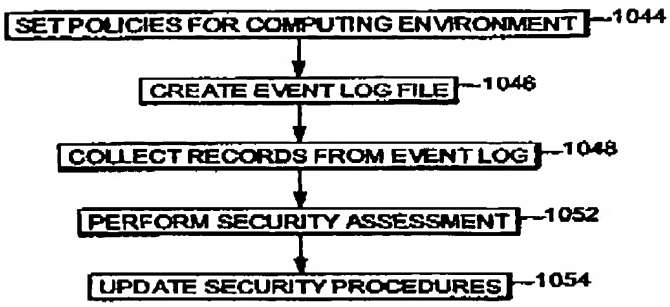

FIG. 10

To one of ordinary skill in the art, the collection of event log files to perform a security assessment is not the same as calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element, as recited by amended Claim 1 of the present application.

In the Office Action, the Examiner admitted that Proctor reference fails to teach or suggest all the features as set forth in amended independent Claim 1. Specifically, the Examiner admits that Proctor fails to teach conducting a discovery scan to identify an element of the computer network and determine the element's functions; scheduling a time to perform the audit scan on the element; and scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan and the security score. For these features, the Examiner relied on the Hartley and Gleichauf references as discussed below.

The Hartley and Gleichauf References

In the Office Action, the Examiner stated that the Proctor reference does not expressly disclose the scheduling feature regarding to the audit scan. For that feature, the Examiner relied on the Hartley reference for disclosing a scheduling module which is used for specifying the time of conducting security modules. Furthermore, the Examiner relied on Gleichauf to teach that the scanning process can be repeated. However, the Hartley and Gleichauf references, either alone or in combination, fail to teach scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan and the security score. Furthermore, the

Hartley and Gleichauf references fail to teach calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element.

The Hartley Reference

As noted above, the Examiner relied on the Hartley reference for disclosing a scheduling module which is used for specifying the time of conducting security modules. In general, the Hartley Reference describes a method and apparatus that can perform a security analysis on a computer system to identify, notify, and possibly correct, vulnerabilities and discrepancies.

However, the Hartley reference fails to teach scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan and the security score, as recited by amended Claim 1 of the present application. Instead, Hartley discloses a schedule module that can provide the functionality to run security checks at predetermined intervals. The checks can be scheduled to run at specific designated times as well as at regular intervals such as monthly or weekly. The schedule module of Hartley can further provide the flexibility to run individual security modules or all tests. See Col. 7, lines 9-14 of the Hartley reference.

Furthermore, in contrast to the invention of amended Claim 1, the Hartley system does not calculate a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element.

The Gleichauf Reference

As noted above, the Examiner relied on the Gleichauf reference to teach that the scanning process can be repeated. In general, the Gleichauf references describes a method and system for adaptive network security using network vulnerability assessment.

However, the Gleichauf reference fails to teach scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan and the security score, as recited by amended Claim 1 of the present application. Instead, Gleichauf discloses a system where as the network information drives the services performed by the security system, the security system is able to configure and reconfigure itself as the network dynamics dictate.

Furthermore, if the system determines that the scanning steps should be repeated, it returns to obtain updated network information, and the method is repeated. See Col. 9, lines 8-13.

Furthermore, in contrast to the invention of amended Claim 1, the Gleichauf system does not calculate a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element.

The Yang, Brabson, and Barroux References

The Examiner further relies on the Yang, Brabson, and Barroux references to teach certain features recited in the dependent claims that rely on Independent Claim 1. However, Applicant further submits that the Yang, Brabson, and Barroux references fail to teach or suggest at least the features as set forth in amended independent Claim 1.

Yang discloses a method and system for priority arbitration in a computer environment having a shared resource capable of servicing a plurality of devices. In one embodiment, Yang can assign an initial priority order to the plurality of devices such that those devices have priorities which are distinct. Next, the system can identify those of the plurality of devices which have issued service requests to the shared resource in a first clock cycle as requesting devices. Provided that there are more than one requesting device in the first clock cycle, the system can select one of the requesting devices to be serviced by the shared resource in a second clock cycle following the first clock cycle, where the selected device has the highest of the priorities among the requesting devices based on the initial priority order. The system can also reassign the priorities among the plurality of devices such that the selected device is assigned the lowest one of the priorities.

Brabson discloses an apparatus and method for reducing resource location traffic in a computer network. The reduction in location traffic is obtained when a node which has initiated a search for a resource which cannot be found starts a timing cycle interval during which subsequent initiating requests at the node are automatically failed without performing the network search. This method can reduce network traffic for searches that are likely to fail. Furthermore, Brabson discloses a threshold counter that alleviates possible difficulties that the above method may cause for high demand resources. The threshold counter can be incremented

each time a search for a specific resource is automatically failed. A network search is performed when either the interval expires or the threshold counter exceeds a threshold count.

Barroux discloses a method and apparatus for automatically surveying a network. The method of surveying a network can include the steps of sending a plurality of SNMP variable value requests via a network where each of the plurality of requests are addressed to a different address in a range of address space; receiving a plurality of replies to the plurality of requests where each of the replies originate from a different address in the range; extracting information from each of the replies where the information characterizing assets at the nodes receiving the plurality of messages and generating the replies; and developing from the extracted information an asset database characterizing a current configuration of assets at the nodes generating the replies.

Summary for Analysis of Independent Claim 1 Rejection

In light of the differences between amended independent Claim 1 and the Proctor, Hartley, and Gleichauf references, Applicant submits that the Proctor, Hartley, and Gleichauf references, either alone or in combination, fail to teach or suggest at least the features as set forth in amended independent Claim 1. Applicant further submits that the Yang, Brabson, and Barroux references and none of the other documents cited by the Examiner teach or suggest those features. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of Claim 1.

Independent Claim 13

The rejection of Claim 13 is respectfully traversed. It is respectfully submitted that the combination of the Proctor, Hartley, and Gleichauf references fails to describe, teach, or suggest: (1) conducting a discovery scan to identify an element of the computer network; (2) configuring an audit scan to perform on the element; (3) scheduling a time to perform the audit scan on the element; (4) running the audit scan at the scheduled time on the element; and (5) calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element, as recited in amended independent Claim 13.

Similar to the analysis of independent Claim 1, the Proctor reference fails to address calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element, as recited in amended independent Claim 13.

In light of the differences between amended independent Claim 13 and the Proctor, Hartley, and Gleichauf references, Applicant submits that the Proctor, Hartley, and Gleichauf references, either alone or in combination, fail to teach or suggest at least the features as set forth in amended independent Claim 13. Applicant further submits that the Yang, Brabson, and Barroux references and none of the other documents cited by the Examiner teach or suggest those features. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of Claim 13.

Independent Claim 22

The rejection of Claim 22 is respectfully traversed. It is respectfully submitted that the combination of the Proctor, Hartley, and Gleichauf references fails to describe, teach, or suggest: (1) receiving an initial scan identifying a network element and the function of the network element; (2) selecting an audit scan to perform on the network element, the selection based on the initial scan, wherein the audit scan is more thorough than the initial scan; (3) scheduling the audit scan to perform on the network element; (4) performing the audit scan on the network element at the scheduled time; (5) receiving data from the selected audit scan of the network element; and (6) computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element, as recited in amended independent Claim 22.

Similar to the analysis of independent Claim 1, the Proctor reference fails to address computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element, as recited in amended independent Claim 22.

In light of the differences between amended independent Claim 22 and the Proctor, Hartley, and Gleichauf references, Applicant submits that the Proctor, Hartley, and Gleichauf references, either alone or in combination, fail to teach or suggest at least the features as set forth

in amended independent Claim 22. Applicant further submits that the Yang, Brabson, and Barroux references and none of the other documents cited by the Examiner teach or suggest those features. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of Claim 22.

Independent Claim 30

The rejection of Claim 30 is respectfully traversed. It is respectfully submitted that the combination of the Proctor and Gleichauf references fails to describe, teach, or suggest: (1) receiving an initial scan identifying a network element; (2) selecting an audit scan to perform on the network element, said selection based on the initial scan; (2) performing the selected audit scan on the network; (3) receiving data from the selected audit scan of the network element; and (4) computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element, as recited in amended independent Claim 30.

Similar to the analysis of independent Claim 1, the Proctor reference fails to address computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element, as recited in amended independent Claim 30.

In light of the differences between amended independent Claim 30 and the Proctor and Gleichauf references, Applicant submits that the Proctor and Gleichauf references, either alone or in combination, fail to teach or suggest at least the features as set forth in amended independent Claim 30. Applicant further submits that the Yang, Brabson, and Barroux references and none of the other documents cited by the Examiner teach or suggest those features. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of Claim 30.

Independent Claim 39

The rejection of Claim 39 is respectfully traversed. It is respectfully submitted that the combination of the Proctor, Hartley, and Gleichauf references fails to describe, teach, or suggest:

(1) the computer network; (2) a security audit system operable for conducting a discovery scan to identify an element of the computer network, configuring and scheduling an audit scan of the element, and computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element; and (3) a console operable for receiving information from the security audit system and transmitting information to the security audit system about the discovery scan and the audit scan, as recited in amended independent Claim 39.

Similar to the analysis of independent Claim 1, the Proctor reference fails to address a security audit system that is operable for computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element, as recited in amended independent Claim 39.

In light of the differences between amended independent Claim 39 and the Proctor and Gleichauf references, Applicant submits that the Proctor and Gleichauf references, either alone or in combination, fail to teach or suggest at least the features as set forth in amended independent Claim 39. Applicant further submits that the Yang, Brabson, and Barroux references and none of the other documents cited by the Examiner teach or suggest those features. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of Claim 39.

Dependent Claims 2-12, 15-21, 23-27, 29, 31-36, 38, and 40-45

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited prior art reference. The Applicants also respectfully submit that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, the Applicants respectfully request that the Examiner withdraw the pending rejections of dependent Claims 2-12, 15-21, 23-27, 29, 31-36, 38, and 40-45.

CONCLUSION

Applicants submit the foregoing as a full and complete response to the Non-Final Office Action dated July 14, 2005. The Applicants and the undersigned thank Examiner Shaw for consideration of these remarks. Applicants submit that this Amendment places the application in condition for allowance and respectfully request such action.

If any issues exist that can be resolved with an Examiner's Amendment or a telephone conference, please contact the undersigned at 404.572.4647.

Respectfully submitted,

Kerry L. Broome

Kerry L. Broome
Reg. No. 54,004

KING & SPALDING LLP
191 Peachtree Street, 45th Floor
Atlanta, Georgia 30303-1763
(404) 572-4600
K&S Docket: 05456.105009